TECNOLOGÍA INFORME

No caiga en esta red de engaños

Se llama phishing, y es una forma fácil de robar la información. Tenga cuidado.

Por **LAURA TAMAYO**

ILUSTRACIÓN **SSTOCK**

De dos a tres minutos. Eso se tarda un ciberdelincuente en hacer una página web idéntica a la de su banco, para que usted, creyendo que es la original, ponga su información y se la roben.

A esa técnica se le conoce como phishing, se pronuncia como la palabra en inglés fishing, que significa pesca o captura. Los hackers hacen campañas y las lanzan como una red a ver quién cae, una estrategia que no es nueva, pero sí muy efectiva. Según explicó *Elie Bursztein,* líder del equipo de investigación de Google, el año pasado en una de sus conferencias de ciberseguridad, el phishing sigue siendo efectivo porque el 45 % de los usuarios de Internet lo ha escuchado, pero no sabe bien en qué consiste.

El phishing no es otra cosa que una suplantación. Los atacantes se hacen pasar por una marca, organismo o institución para robar datos personales. Una cadena en WhatsApp, un correo con una oferta llamativa, un artículo en Facebook que aparece mágicamente y tiene muchos likes y hasta un producto llamativo en Instagram. Los métodos son tan efectivos que el año pasado el 78 % de los problemas de seguridad en Estados Unidos se lograron gracias a estas campañas, reportó el informe de seguridad de la compañía de telefonía móvil Verizon.

Para no ser víctima de una técnica que nació hace ya 30 años, mire las ingeniosas campañas que han descubierto recientemente firmas de ciberseguridad y cómo logran capturar su información.

¿Cómo reconocerlo?

Una de las campañas más recientes en Colombia, analizada por la firma de ciberseguridad Eset, consistió en usar la imagen de Netflix para hacer un correo electrónico muy parecido a los que ellos suelen enviar a sus clientes, solo que este pedía actualizar la información de la cuenta.

"Si no actualiza la información en las próximas 72 horas, limitaremos lo que puede hacer con su cuenta", advertía el supuesto correo y tenía un botón que decía "verificar ahora".

El engaño estaba precisamente en que el correo venía de un dominio que decía "@policypla", y dirigía a una página que no era netflix.com sino algo como "netflix.webformu...".

Aunque los mismos navegadores suelen alertar de que los sitios no parecen seguros, las personas acceden, actualizan sus datos bancarios y los cibercriminales los roban. *David Pereira*, experto en ciberseguridad y gerente de SecPro, en una demostración para EL COLOMBIANO evidencia lo rápido que se pueden diseñar esos sitios idénticos y cómo se capturan las contraseñas.

La demora entonces es que usted como usuario se tome el trabajo de revisar dos veces el dominio de una página de promociones y la procedencia de un correo electrónico, y así no caiga en el engaño. Las diferencias pueden ser sutiles: en lugar de decir netflix.com aparece netflix.co. Según el índice anual de inteligencia de amenazas 2020, publicado por IBM, los atacantes van detrás de datos monetizables, por eso el 60 % de las marcas falsificadas son de Google y YouTube; Apple (el 15 %) y Amazon (12 %); Facebook, Instagram y Netflix en menor medida.

El phishing sigue siendo efectivo porque el 45 % de los usuarios de Internet lo ha escuchado, pero no sabe bien en qué consiste.

ELIE BURSZTEIN
Líder de investigación de Google

No se ve la diferencia

El año pasado Google aseguró que bloqueó 100 millones de correos maliciosos en Gmail por día, pero una investigación de la firma de ciberseguridad Kaspersky concluyó que el phishing aumentó 9,5 % en el último trimestre de 2019. Los hackers no solo se aprovechan de fechas como Black Friday y Cyber Monday sino que ya han desarrollado técnicas para que los enlaces de las páginas se vean como los originales.

Se llaman ataques homográficos. *Camilo Gutiérrez,* jefe del laboratorio de investigación de la firma de ciberseguridad ESET para Latinoamérica, aclara que consiste en usar letras de otros alfabetos dentro de la url para que se vean similares. "Hay una letra del alfabeto cirílico que es exactamente igual a la L, entonces mezclan caracteres de diferentes alfabetos para que las palabras se vean similares", explica.

Pereira muestra cómo revisar los certificados de los sitios. Revisarlo le tomará un minuto más. Haga clic en el candado y vaya a donde dice certificado. No basta que aparezca "válido", porque hay personas que se dedican a vender ese tipo códigos. Ahí es donde los ciberdelincuentes aprovechan para suplantar sitios. Presione donde dice certificado y verifique que haya sido emitido para la empresa de la página web que está buscando. Pereira recomienda descargar la herramienta gratuita Netcraft Toolbar para instalarla como una extensión en su navegador. Esta le da un indicador de qué tan confiables son las páginas que visita. Si aparece todo en verde, puede entrar más tranquilo.

Hasta el coronavirus

En otra campaña los hackers se hicieron pasar por el Ministerio de Salud del país y enviaron correos diciendo: "Detectamos en su sector la presencia de CoVid-19, adjuntamos un archivo pdf con las claves".

La información fue desmentida por MinSalud el pasado 5 de marzo, un día antes de que se confirmara el primer caso en el país. Lo que buscan ahí los ciberatacantes es que los usuarios descarguen un archivo con código malicioso para tomar el control de la máquina, un escenario que resulta más peligroso.

Tenga cuidado: ni porque le ofrezcan ver todas las películas nominadas a los Oscar en alta definición y español o le prometan con el 90 % de descuento el bloqueador que tanto ha estado buscando, dé clic. Le toma poco tiempo verificar para no caer en estas redes fraudulentas ■

CLAVES

PARA CUIDARSE DE ESTA TÁCTICA

1. Evite abrir enlaces que le lleguen directamente a su correo electrónico o número de celular.
2. Los atacantes son expertos en persuasión, desconfíe de rebajas escandalosas o del "si no lo hace en 30 minutos".
3. Active el doble factor de autenticación en sus cuentas. Eso puede detener a un atacante que entra con info robada.
4. Siempre verifique el dominio de los correos que recibe y le invitan a descargar cosas o seguir enlaces.

EN DEFINITIVA

Desconfíe de esas ofertas en las que le prometen un descuento maravilloso o que lo amenazan con no conseguir la oferta si no responde en 30 minutos. Contra el phishing hay que cuidarse.